Deutscher Bundestag **Drucksache 18/707**

18. Wahlperiode 05.03.2014

Antwort
der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Wolfgang Gehrcke, Annette Groth, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/540 –**

Computergestütztes Aufspüren von unerwünschtem Verhalten im öffentlichen Raum

Vorbemerkung der Fragesteller

Die Industrie hat mittlerweile zahllose „Sensoren“ entwickelt, mit denen der öffentliche Raum überwacht werden kann. Hierzu gehören Videokameras, die mittlerweile in einer neuen Generation montiert werden und hochauflösende Bilder liefern sowie neuere bildgebende Verfahren (das sogenannte Maschinensehen). Hinzu kommen Mikrofone und Bewegungsmelder, aber auch Gasdetektoren zum Aufspüren gefährlicher Stoffe oder erhöhten Alkoholgehalts im Fußballstadion. Für die Verarbeitung der Daten werden große Kapazitäten benötigt. Hier sollen computergestützte Verfahren abhelfen. So können als „verdächtig“ eingestufte Bewegungsabläufe, Geräusche oder Gerüche herausgefiltert werden. Im Falle eines „Treffers“ erhält der Bediener eine Ereignismeldung. Vor einigen Jahren ist hierzu das EU-Forschungsprogramm INDECT bekannt geworden. Dessen Teilnehmerinnen und Teilnehmer entwickeln eine Plattform, um Bilder aus der Videoüberwachung mit Polizeidatenbanken und dem Internet abzugleichen. Berechtigterweise hat das in diesem Sommer endende Projekt viel Kritik auf sich gezogen: Bürgerrechtsgruppen und Netzaktivisten hatten INDECT als „Bevölkerungsscanner“ kritisiert (Bundestagsdrucksache 17/3940). Mehrere Polizeibehörden interessieren sich für das Ergebnis von INDECT, das ebenfalls beteiligte Bundeskriminalamt (BKA) war allerdings ausgestiegen – angeblich wegen des „umfassenden Überwachungsgedankens“ (Pressemitteilung, 13. Oktober 2011).

Nun finanziert die Europäische Kommission weitere Forschungsvorhaben mit ähnlicher Zielsetzung. Wieder steht die Auswertung möglichst vieler Quellen im Mittelpunkt, darunter neben der Überwachung öffentlicher Orte auch soziale Medien. Die Plattformen sollen polizeilich relevante Vorfälle auch vorhersagen. Eines der neueren EU-Programme trägt den Namen PROACTIVE (www.fp7-proactive.eu). Der Name markiert einen neuen Trend in der Strafverfolgung: Im Gegensatz zu „Prävention“ soll die „proaktive Verbrechensbekämpfung“ greifen, wenn die vermeintliche Bedrohung noch gar nicht in Sicht ist. Damit schlägt sich das Konzept von „Gefährdern“ bzw. „Gefahrengebieten“ nach Ansicht der Fragesteller auch in der Sicherheitsforschung nie-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 3. März 2014 übermittelt und mit Schreiben vom 30. April 2014 korrigiert (vgl. Drucksache 18/1409).

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

der. Die Rede ist von „vorhersagenden Schlussfolgerungen und der Einbindung mehrerer Quellen“, als Ziel wird eine „Verhinderung terroristischer Angriffe in städtischer Umgebung“ ausgegeben. Im Originaltitel wird das Wort „Fusion“ benutzt. Gemeint ist die statistische Auswertung polizeilicher Daten in Verbindung mit Informationen von „Sensoren“, die über die ganze Stadt verteilt sein können. Besondere Aufmerksamkeit wird aber dem „Internet der Dinge“ zuteil. Gewöhnlich werden damit technische Alltagshelfer bezeichnet, die über eine Netzwerkverbindung verfügen. In PROACTIVE sollen sie der Polizei zur Verhaltenskontrolle ihrer Nutzerinnen und Nutzer dienen. Diese Art des Zusammenführens von Daten mehrerer Quellen ist in Deutschland derzeit allerdings nur im Rahmen von Ermittlungen gestattet. Die Europäische Union (EU) finanziert deshalb rechtliche und ethische Forschungen, um die Gesetzeslage in den Mitgliedstaaten zu analysieren und mit den neuen Technologien zu synchronisieren (www.smartsurveillance.eu). PROACTIVE wird angeführt vom italienischen Konzern Vitrociset, der auf zivile und militärische Überwachungs- und Transportsysteme spezialisiert ist. Ebenfalls an Bord ist die polnische University of Science and Technology mit Sitz in Krakau, deren Forscher bereits an INDECT geforscht hatten. Unter den Beteiligten findet sich aber auch die Universität der Bundeswehr München. Die kurze Beschreibung über die Mitarbeit der deutschen Militärforscher lässt darauf schließen, dass die in PROACTIVE entwickelte Plattform auch Drohnen einbinden könnte – oder aber deren autonome Fähigkeit, schnell Entscheidungen zu treffen. Zuständig ist das Institut für Flugsysteme, dessen Arbeiten zur künstlichen Intelligenz unbemannter Luftfahrzeuge durch PROACTIVE gelobt werden. Diese seien geeignet, eine Situation schnell einzuschätzen und Entscheidungshilfen zu geben. Für die Anwendung von PROACTIVE interessieren sich Polizeibehörden und Geheimdienste aus Finnland, Zypern, Ungarn, Rumänien und Polen, aber auch das in Italien ansässige Crime and Justice Research Institute (UNICRI). Das UNICRI ist bei den Vereinten Nationen angesiedelt und beschäftigt sich insbesondere mit Forschungen zur Beherrschbarkeit von Sportereignissen oder Gipfelprotesten. Auch das Bayerische Landeskriminalamt (BLKA) hat mindestens zweimal an Workshops von „Endnutzern“ teilgenommen (www.fp7-proactive.eu/latest-news/conclusions-2nd-end-users-advisory-board).

Während sich PROACTIVE mit „terroristischen Angriffen“ befasst, soll das EU-Programm CAPER die „organisierte Kriminalität“ proaktiv adressieren (www.cordis.europa.eu/projects/rcn/99655_en.html). Der Titel lässt sich als „Gemeinschaftliche Information, Beschaffung, Verarbeitung, Verwertung und Meldung zur Vorbeugung organisierter Kriminalität“ übersetzen. Das System soll Informationstechnologie ausforschen und auswerten. Hierzu gehört insbesondere die „Open Source Intelligence“ (OSINT) des Internets. Gemeint sind öffentlich zugängliche Daten von Webseiten und Sozialen Medien. Angeführt vom auf Sicherheitsanwendungen spezialisierten Softwarehaus S21sec macht auch das Fraunhofer-Institut für Graphische Datenverarbeitung IGD bei CAPER mit. Das Institut erklärt zur Funktionsweise der Plattform, die gewonnenen Daten würden „semantisch analysiert und visuell so aufbereitet, dass Zusammenhänge oder besondere Ereignisse erkannt werden können“. CAPER will Informationen von Diensten wie Twitter mit „Close Source Intelligence“ verbinden. Hinter dem Begriff verbergen sich auch Informationen, die in Polizeidatenbanken lagern. Diese polizeilichen Daten könnten dann mit Analysesystemen verknüpft werden, die Bilder, Videos, verschiedene Sprachen und biometrische Daten verarbeiten. CAPER soll diese Rasterfahndung in verschiedenen Datenquellen derart vereinfachen, dass sie über ein simples Interface vorgenommen werden kann. Auf diese Weise wollen die Ermittler bislang unentdeckte Informationen finden. Schon seit Beginn waren die israelische Polizei und die Mossos d’Esquadra aus Barcelona als „Endnutzer“ von CAPER registriert. Als neue Beobachter sind nun das britische Innenministerium, der rumänische Geheimdienst und das deutsche BKA an Bord (www.fp7-caper.eu/consortium. html). Dies ist also mindestens das zweite Vorhaben, in dem sich die Kriminalisten aus Wiesbaden mit dem Blick in die Glaskugel befassen (Bundestagsdrucksache 17/13441).

1. Hinsichtlich welcher Forschungsprojekte sind welche Bundesbehörden des Innern, der Verteidigung oder des Bundeskanzleramtes mit der Verbesserung von automatisierten Verfahren des „Data Mining“, der Verarbeitung von „Massendaten“ in (nahezu) Echtzeit, der „Prediktiven Analyse“, „vorhersagenden Schlussfolgerungen“, der Ausgabe von kriminalistischen „Hypothesen“ oder der computergestützten Auswertung von sozialen Medien (darunter Twitter, Facebook) als Teilnehmende, Beobachterinnen oder auch als Adressatinnen entsprechender Berichte auf deutscher Ebene befasst?

   a) Um welche Projekte handelt es sich dabei konkret, und wer nimmt daran (auch zur Beobachtung) teil?

Das Bundesministerium der Verteidigung (BMVg) ist mit einem Forschungsvorhaben zur Wissenserschließung aus offen Quellen (WeroQ, Vorhabennummer EF020) befasst. Soziale Medien sind davon ausgenommen und werden nicht betrachtet. An diesem Vorhaben sind keine weiteren Teilnehmer und Beobachter beteiligt.*

   b) Welche Beiträge haben private Firmen oder Institute hierfür erbracht?

Hauptauftragnehmer des Projekts des BMVg ist die Fraunhofer Gesellschaft, Forschungsinstitut für Kommunikation, Informationsverarbeitung und Ergonomie (FhG FKIE) und im Unterauftrag die IBM mit ihrem Produkt IBM Content Analytics.

   c) Wann wurden die Projekte begonnen, wann enden sie, welches Finanzvolumen haben sie, und wie werden sie finanziert?

Geplanter Leistungszeitraum ist der 2. Mai 2014 bis 31. Dezember 2016 mit einem Haushaltsmittelansatz in Höhe von 1,35 Mio. Euro.

   d) Welche Plattformen mit welchen gewünschten Funktionsweisen sollen die einzelnen Vorhaben entwickeln?

Bei Erfolg werden die Ergebnisse in ein Führungsinformationssystem der Bundeswehr überführt.

2. Hinsichtlich welcher Forschungsprojekte sind welche Bundesbehörden des Innern, der Verteidigung oder des Bundeskanzleramtes mit der Verbesserung von automatisierten Verfahren des „Data Mining“, der Verarbeitung von „Massendaten“ in (nahezu) Echtzeit, der „Prediktiven Analyse“, „vorhersagenden Schlussfolgerungen“, der Ausgabe von kriminalistischen „Hypothesen“ oder der computergestützten Auswertung von sozialen Medien (darunter Twitter, Facebook) als Teilnehmende, Beobachterinnen oder auch als Adressatinnen entsprechender Berichte auf Ebene der EU befasst?

Das Bundeskriminalamt (BKA) nimmt als Beobachter im Gaststatus an dem im 7. Forschungsrahmenprogramm der Europäischen Union (EU) geförderten Projekt CAPER (Collaborative information, Acquisition, Processing, Exploitation and Reporting for the prevention of organised crime) teil. Die Bundespolizei (BPOL) hat als Beobachter im Gaststatus an einer Projektveranstaltung von CAPER teilgenommen.

---

* Korrektur siehe Drucksache 18/1409

a) Um welche Projekte handelt es sich dabei konkret, und wer nimmt daran (auch zur Beobachtung) teil?

Das BKA hat das Projekt CAPER in der Eigenschaft als Beobachter im Gaststatus durch einen Mitarbeiter begleitet (siehe hierzu auch die Antworten zu den Fragen 13 ff.). Die BPOL hat bisher einmalig in der Eigenschaft als Beobachter im Gaststatus an einer Projektveranstaltung teilgenommen.

Nähere Projektinformationen sind im Internet unter www.fp7-caper.eu einsehbar.

b) Welche Beiträge haben private Firmen oder Institute hierfür erbracht?

Zum Projekt CAPER sind dem BKA und der BPOL über die öffentlich einsehbaren Beiträge hinausgehende Beiträge der Konsortialpartner aufgrund des eingeschränkten Gast-/Beobachterstatus nicht bekannt.

c) Wann wurden die Projekte begonnen, wann enden sie, welches Finanzvolumen haben sie, und wie werden sie finanziert?

Das Projekt CAPER wurde am 1. Juli 2011 mit einem Finanzierungsrahmen von rd. 7,1 Mio. Euro begonnen, wovon die Europäische Kommission rd. 5,6 Mio. Euro zur Verfügung stellt (siehe auch die Antwort zu Frage 13).

Weitere Projektrahmendaten sind der Projektwebsite unter www.fp7-caper.eu sowie der dort hinterlegten Projektbroschüre zu entnehmen.

d) Welche Plattformen mit welchen gewünschten Funktionsweisen sollen die einzelnen Vorhaben entwickeln?

Im Rahmen des Projektes CAPER soll ein automatisiertes datenbankgestütztes Tool zur Datensammlung, Auswertung, Analyse und visuellen Darstellung von öffentlich zugänglichen sog. Open-Source-Informationen (u. a. aus Suchmaschinen und sozialen Netzwerken) als Prototyp für die Strafverfolgung (insbesondere im Rahmen der Bekämpfung der organisierten Kriminalität) sowie für besondere Gefahrenabwehranlässe entwickelt werden (siehe die Antwort zu Frage 2a).

3. Inwiefern setzen welche Bundesbehörden des Innern, der Verteidigung oder des Bundeskanzleramtes die automatisierten Verfahren des „Data Mining“, der Verarbeitung von „Massendaten“ in (nahezu) Echtzeit, der „Prediktiven Analyse“, „vorhersagenden Schlussfolgerungen“, der Ausgabe von kriminalistischen „Hypothesen“ oder der computergestützten Auswertung von sozialen Medien (darunter Twitter, Facebook) bereits ein?

Hinsichtlich des Bundesnachrichtendienstes (BND) kann die Beantwortung der Frage 3 nicht offen erfolgen, da die erbetenen Auskünfte Informationen zu Aufklärungsaktivitäten, Analysemethoden und zur aktuellen Aufgabenerfüllung des BND preisgeben. Arbeitsmethoden und Vorgehensweisen des BND sind im Hinblick auf die künftige Auftragserfüllung besonders schutzbedürftig, ihre Veröffentlichung ließe Rückschlüsse auf die Fähigkeiten, Methoden und Aufklärungsschwerpunkte zu. Eine Veröffentlichung von Einzelheiten betreffend solche Fähigkeiten würde zu einer wesentlichen Schwächung der den Nachrichtendiensten zur Verfügung stehenden Möglichkeiten zur Informationsgewinnung führen. Dies könnte die Effektivität der nachrichtendienstlichen Aufklärung beeinträchtigen, was wiederum für die Interessen der Bundesrepublik Deutschland schädlich sein kann. Deshalb sind die entsprechenden Informationen als Verschlusssache gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen

Schutz von Verschlusssachen (VS-Anweisung – VSA) mit dem VS-Grad „VS-Vertraulich“ eingestuft. Die Informationen können in der Geheimschutzstelle des Deutschen Bundestages eingesehen werden. Das Bundesministerium des Innern hat die Antwort als „VS – Vertraulich“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

4. Inwiefern haben sich auch Bundesbehörden bereits mit Verfahren befasst oder setzen sie bereits ein, wie sie unter anderem „DER SPIEGEL“ über den britischen Geheimdienst GCHQ berichtete und wonach dieser in Echtzeit verfolgen kann, welche Videos auf YouTube angesehen werden, welche Inhalte auf Facebook ein „Gefällt mir“ bekommen, und welche Seiten auf Googles Blogplattform Blogger.com gelesen werden (SPIEGEL ONLINE, 28. Januar 2014)?

Bundesbehörden haben sich bisher nicht mit solchen Verfahren befasst und setzen sie auch nicht ein.

a) Über welche eigenen Erkenntnisse verfügt die Bundesregierung hinsichtlich des Programms „Squeaky Dolphin“ oder ähnlicher Verfahren der US-amerikanischen National Security Agency (NSA) oder des GCHQ zur Social-Media-Analyse, deren Namen noch nicht öffentlich bekannt sind?

Zu solchen Programmen liegen der Bundesregierung keine Informationen vor.

b) Was ist der Bundesregierung über Möglichkeiten bekannt, Daten, die von Smartphone-Apps übertragen werden und die persönliche Informationen enthalten, abzuhören?

Alle Daten, die von Smartphone-Apps unverschlüsselt oder unsicher verschlüsselt übertragen werden, können grundsätzlich inhaltlich erschlossen werden. Dies ist jedem möglich, der unmittelbaren Zugriff auf die Übertragungswege hat und über die entsprechende Erfassungstechnik verfügt.

5. Welchen Namen tragen die „integrierte[n] Fachanwendungen zur Erfassung und Aufbereitung der im Rahmen einer Telekommunikationsüberwachung aufgezeichneten Daten der Hersteller Syborg und DigiTask“ bei Polizeibehörden des Bundes, die laut der Bundesregierung „aufgezeichneten Rohdatenstrom […] in lesbarer Form zur Verfügung stell[en]“ (Bundestagsdrucksachen 17/14739 und 17/14530), und von welchen Abteilungen deutscher Bundesbehörden werden diese genutzt?

Das BKA und die BPOL nutzen die Fachanwendung „Syborg Interception Center (SIC)“ der Firma Syborg Informationssysteme GmbH. Produkte der Firma DigiTask werden weder bei der BPOL noch beim BKA verwendet.

Zur Erfassung und Aufbereitung der im Rahmen einer Telekommunikationsüberwachung aufgezeichneten Daten nutzt der Zollfahndungsdienst integrierte Fachanwendungen der Firma DigiTask GmbH (DigiTask Lawful Interception Center).

Der Zollfahndungsdienst verwendet für die in Rede stehenden Zwecke keine Produkte der Firma Syborg.

6. Inwiefern haben Bundesbehörden jemals von Diensten der EU-Polizeiagentur Europol Gebrauch gemacht, die eine Auswertung von „Open Source Intelligence“ anbietet und dies im „Europol Work Programme 2014“ als „provision of tailored newsfeeds on cybercrime trends, technological developments and other relevant information“ und „permanent Open Source scanning capability“ bewirbt?

Soweit in der Kürze der zur Verfügung stehenden Zeit recherchierbar, hat keine Bundesbehörde von den in der Frage 6 genannten Diensten der EU-Polizeiagentur Europol Gebrauch gemacht.

7. Auf welche Weise soll das EU-Programm PROACTIVE „terroristische Angriffe in städtischer Umgebung“ verhindern?

   a) Wer nimmt daran (auch zur Beobachtung) teil, welche Beiträge haben private Firmen oder Institute hierfür erbracht, wann wurde das Projekt begonnen, wann endet es, welches Finanzvolumen hat es, und wie wird es finanziert?

   b) Auf welche Weise sollen bei PROACTIVE „vorhersagende Schlussfolgerungen“ erzielt werden?

   c) Welche „Quellen“ werden hierfür eingebunden?

   d) Was ist damit gemeint, wenn bei PROACTIVE auch die Überwachung über das „Internet der Dinge“ beforscht wird?

Das im Rahmen der Sicherheitsforschung des 7. EU-Forschungsrahmenprogramms geförderte Projekt „PROACTIVE - Predictive reasoning and multisource fusion empowering anticipation of attacks and terrorist actions in urban environments“ läuft vom 1. Mai 2012 bis zum 30. April 2015. Das Projekt hat ein Finanzvolumen von 4 679 412 Euro und wird seitens der Europäischen Kommission mit 3 371 799 Euro gefördert. Folgende Partner werden gefördert:

- Vitrociset SPA, Italien
- Akademia Gorniczo-Hutnicza im. Stanislawa Staszica W Krakowie, Polen
- Research and Education Laboratory in Information Technologies, Griechenland
- Consorzio Milano Ricerche, Italien
- HW Communications Limited, Vereinigtes Königreich
- Center for Security Studies, Griechenland
- Kingston University Higher Education Corporation, Vereinigtes Königreich
- Istituto di Sociologia Internazionale di Gorizia I.S.I.G, Italien
- Magyar Tudomanyos Akademia Szamitastechnikai es Automatizalasi Kutato Intezet, Ungarn
- Universität der Bundeswehr München, Deutschland.

Weitere Informationen zu laufenden Projekten sind in der Projektdatenbank der Europäischen Kommission (CORDIS) enthalten.

8. Inwiefern ist eine bei PROACTIVE beforschte „proaktive Verbrechensbekämpfung“ auf Basis der Analyse technischer „Sensoren“ in Deutschland rechtlich durchführbar, bzw. welche Gesetzesänderungen wären hierfür notwendig?

Bei PROACTIVE handelt es sich um ein laufendes Forschungsvorhaben, dessen Ergebnisse für 2015 erwartet werden. Die Bundesregierung hat die Vereinbarkeit einer Einführung von entsprechenden Technologien mit deutschem oder europäischem Recht nicht geprüft.

9. Wie bewertet die Bundesregierung die Notwendigkeit von PROACTIVE?

Das 7. Forschungsrahmenprogramm ist ein Programm der EU. Die Durchführung obliegt der Europäischen Kommission, die auch die fachliche Bewertung und Auswahl von Projektvorschlägen vornimmt.

10. Worin besteht der Beitrag der Universität der Bundeswehr München sowie des Instituts für Flugsysteme in München bei PROACTIVE?

    a) Auf welche bereits vorliegenden Ergebnisse früherer Forschungen wird dabei zurückgegriffen?

Das Institut für Flugsysteme der Universität der Bundeswehr München befasst sich mit Grundlagenforschung im Bereich der Automatisierung, der Mensch-Maschine-Interaktion sowie der Sensorik von Luftfahrzeugen.

    b) Welche eigenen, ähnlichen Forschungen betreiben die Universität der Bundeswehr München sowie das Institut für Flugsysteme?

Auf die Antwort zu den Fragen 10 und 10a wird verwiesen.

    c) Inwiefern wird bei PROACTIVE auch die Einbindung von Drohnen beforscht, und welche Beiträge liefert die Bundeswehr hierfür?

In PROACTIVE wird durch das Institut für Flugsysteme der Universität der Bundeswehr die Integration eines mobilen fliegenden Sensorknotens untersucht.

11. Welche konkreten Beiträge haben Polizeibehörden und Geheimdienste aus Finnland, Zypern, Ungarn, Rumänien und Polen nach Kenntnis der Bundesregierung bei PROACTIVE erbracht?

    a) Wie haben diese anvisierten „Endnutzer“ vorab ihren „Bedarf“ definiert?

    b) Auf welche Weise wären die Forschungen der Universität der Bundeswehr München sowie des Instituts für Flugsysteme geeignet, die Bedarfe der „Endnutzer“ zu erfüllen?

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

12. Was ist der Bundesregierung durch die Mitarbeit der Bundeswehr oder durch eigene Erkenntnisse über die Teilnahme des BLKA an PROACTIVE bekannt?

    a) Welchen Beitrag hat das BLKA im Projekt erbracht, bzw. welches Interesse hat die Behörde vorgetragen?

    b) Inwiefern steht das BLKA hierzu in Kontakt mit der Universität der Bundeswehr München oder dem Institut für Flugsysteme?

    c) An welchen Workshops von „Endnutzern“ hat das BLKA nach Kenntnis der Bundesregierung teilgenommen, und welche Themen wurden dort behandelt?

Antwort zu Frage 12b

Zwischen der Universität der Bundeswehr München und dem BLKA besteht keine direkte Zusammenarbeit. Ein Kontakt besteht über das Konsortium des EU-Projekts PROACTIVE „terroristische Angriffe in städtischer Umgebung“.

Antwort zu den Fragen 12, 12a und 12c

Zu den übrigen Fragestellungen liegen der Bundesregierung keine Erkenntnisse vor.

13. Auf welche Weise soll das EU-Programm CAPER die „organisierte Kriminalität“ proaktiv adressieren?

Das im Rahmen der Sicherheitsforschung des 7. EU-Forschungsrahmenprogramms geförderte Projekt „CAPER - Collaborative information, acquisition, processing, exploitation and reporting for the prevention of organised crime“ läuft vom 1. Juli 2011 bis zum 30. Juni 2014. Das Projekt hat ein Finanzvolumen von 7 166 700 Euro und wird seitens der Europäischen Kommission mit 5 579 346 Euro gefördert. Weitere Informationen zu diesem Projekt sind in der Projektdatenbank der Europäischen Kommission (CORDIS) und auf der Website www.fp7-caper.eu enthalten. Zum Ziel des Forschungsprojekts vgl. die Antworten zu den Fragen 2 und 13b bis f.

a) Wer nimmt daran (auch zur Beobachtung) teil, welche Beiträge haben private Firmen oder Institute hierfür erbracht, wann wurde das Projekt begonnen, wann endet es, welches Finanzvolumen hat es, und wie wird es finanziert?

Folgende Partner werden gefördert:

- S21Sec Information Security Labs S.L., Spanien
- Fundacion Centro de Tecnologias de Interaccion Visual y Comunicaciones Vicomtech, Spanien
- Fraunhofer-Institut für Graphische Datenverarbeitung, Deutschland
- Synthema S.R.L., Italien
- Voiceinteraction – Tecnologias de Processamento da Fala, SA, Portugal
- Altic SARL, Frankreich
- Technion – Israel Institute of Technology, Israel
- Alma Consulting Group SAS, Frankreich
- Angel Iglesias S.A. – IKUSI, Spanien
- Consiglio Nazionale Delle Ricerche, Italien

- Universitat Autonoma de Barcelona, Spanien
- Studio Professionale Associaton a Baker & McKenzie, Italien
- Ministero Dell'Interno, Italien
- Ministério da Justiça, Portugal
- Guardia Civil Espanola, Spanien
- Departament d'Interior – Generalitat de Catalunya, Spanien
- Ministry of Public Security, Israel.

Das BKA ist mit einem Mitarbeiter als Beobachter im Gaststatus an ausgewählten Projektsitzungen beteiligt.

b) Auf welche Weise sollen bei CAPER die „gemeinschaftliche Information, Beschaffung, Verarbeitung, Verwertung und Meldung" von Informationen optimiert werden?

c) Auf welche Weise sollen nach Kenntnis der Bundesregierung bei CAPER Inhalte „semantisch analysiert und visuell so aufbereitet werden, dass Zusammenhänge oder besondere Ereignisse erkannt werden können"?

Im Rahmen des Forschungsprojekts CAPER sollen ein Machbarkeitsnachweis sowie eine prototypische Implementierung erfolgen. Eine Analyse und Bewertung von Einsatzszenarien, semantischen Analysemöglichkeiten sowie visuellen Aufbereitungen können erst nach dem Ende des Projekts erfolgen.

d) Auf welche Weise soll hierfür „Open Source Intelligence" genutzt werden?

Die im Projekt CAPER zu analysierenden Daten stammen aus unterschiedlichen „Open Source-Quellen" wie z. B. Suchmaschinen oder Daten aus frei zugänglichen sozialen Netzwerken.

e) Auf welche Weise sollen auch Kurznachrichtendienste eingebunden werden?

Ob im Rahmen des Projekts eine protoypische Implementierung von Kurznachrichtendiensten erfolgt, ist der Bundesregierung nicht bekannt.

f) Auf welche Weise sollen bei CAPER auch Informationen einer „Close Source Intelligence" eingebunden werden, und welche sind damit konkret gemeint?

Eine Integration von anderen als „Open Source-Informationen", z. B. Informationen aus anderen Systemen (closed source) ist im Projekt konzeptionell vorgesehen. Inwieweit eine prototypische Realisierung in der Restprojektlaufzeit erfolgt, ist der Bundesregierung nicht bekannt.

14. Worin besteht nach Kenntnis der Bundesregierung der Beitrag des Fraunhofer-Instituts für Graphische Datenverarbeitung IGD bei CAPER?

Die Forschungsarbeiten des Fraunhofer IGD in CAPER gelten dem Bildvergleich und der Visualisierung der erhaltenen Daten. Personen in Bildern und Videos zu erkennen, soll es Ermittlungsbehörden ermöglichen, die Beziehungen innerhalb von Mafiastrukturen auch auf diesem Wege nachzuvollziehen. Über eine gut erfassbare Visualisierung sollen dabei die Daten, die sich aus der Ermittlung ergeben, für die Polizei schneller zu verstehen sein. Zudem realisiert

das Fraunhofer IGD auch die technische Umsetzung der Vorgaben sowohl für den Datenschutz als auch für den Schutz der Persönlichkeitsrechte.

Auf welche bereits vorliegenden Ergebnisse früherer Forschungen wird dabei nach Kenntnis der Bundesregierung zurückgegriffen?

Das 1987 gegründete Fraunhofer IGD erforscht Technologien und Anwendungen, die auf Visual Computing aufbauen. Dieses Technologiefeld erfasst, bearbeitet und verwendet Bilder und Graphiken für alle denkbaren computerbasierten Anwendungen. Die Erfahrung aus zahlreichen Forschungsprojekten bildet die Grundlage für die aktuellen Forschungen des Fraunhofer IGD.

15. Welche konkreten Beiträge haben die israelische Polizei, die Mossos d'Esquadra aus Barcelona, das britische Innenministerium und der rumänische Geheimdienst bei CAPER erbracht?

    a) Wie haben diese anvisierten „Endnutzer" vorab ihren „Bedarf" definiert?

    b) Auf welche Weise wären die Forschungen bei CAPER geeignet, die Bedarfe der „Endnutzer" zu erfüllen?

Der Bundesregierung liegen hierzu keine Informationen vor.

16. Aus welchem Grund interessiert sich das BKA für die Mitarbeit bei CAPER?

    a) Auf welche Weise ist das BKA als Teilnehmer aufgenommen worden, und wer hatte einen entsprechenden Antrag gestellt?

    Welchen Beitrag hat das BKA im Projekt erbracht, bzw. welches Interesse hat die Behörde vorgetragen?

Das BKA ist kein Projektteilnehmer im CAPER-Projekt. Das BKA ist nur als Beobachter im Gaststatus an ausgewählten Projektsitzungen beteiligt. Konkrete Beiträge, die über eine Beteiligung im Rahmen der Projektsitzungen hinausgehen, wurden nicht erbracht.

Ziel der Projektbeobachtung ist die Feststellung der Funktionalität des im Projekt avisierten Prototyps als Grundlage einer Bewertung im Hinblick auf eine mögliche Unterstützung bei der Aufgabenerfüllung innerhalb der BKA-Zuständigkeit.

b) Inwiefern steht das BKA hierzu in Kontakt mit dem Fraunhofer-Institut für Graphische Datenverarbeitung IGD?

Im Rahmen des CAPER-Projekts beschränkt sich der Kontakt auf die Teilnahme an ausgewählten Projektsitzungen.

c) An welchen Workshops von „Endnutzern" hat das BKA teilgenommen, und welche Themen wurden dort behandelt?

Außerhalb der besuchten Projektsitzungen ist keine Teilnahme an Workshops von „Endnutzern" erfolgt.

17. Inwiefern ist eine bei CAPER beforschte „proaktive Verbrechensbekämpfung“ in Deutschland rechtlich durchführbar, bzw. welche Gesetzesänderungen wären hierfür notwendig?

Die Bundesregierung kennt bisher keine Projektergebnisse. Sie hat die Vereinbarkeit einer Einführung von entsprechenden Technologien mit deutschem oder europäischem Recht nicht geprüft.

18. Wie bewertet die Bundesregierung die Notwendigkeit von CAPER?

Das 7. Forschungsrahmenprogramm ist ein Programm der EU. Die Durchführung obliegt der Europäischen Kommission, die auch die fachliche Bewertung und Auswahl von Projektvorschlägen vornimmt.

19. Was ist das Ziel des Projekts „DRiving InnoVation in Crisis Management for European Resilience“ (Driver), an dem laut eigener Aussage auch das Deutsche Zentrum für Luft- und Raumfahrt e. V. (DLR) beteiligt ist (www.dlr.de vom 4. Juli 2013)?

Es handelt sich um einen Projektvorschlag für ein Demonstrationsprogramm für das Krisenmanagement: Erdbeben, Hochwasser, Sturm und technische Katastrophen können weite Flächen beeinträchtigen. Um Hilfe für die Betroffenen zu ermöglichen, ist eine genaue Kenntnis der Schäden und der Ereignisse vor Ort wichtig. Es sollen Technologien für das Krisenmanagement im Katastrophenfall entwickelt werden, so dass unbemannte Luftfahrzeuge die Lage aus der Luft mit Kameras und weiteren Messsonden erfassen und so einen entscheidenden Beitrag bei der Katastrophenhilfe leisten können; Helfer müssen im Katastrophenfall schnell auf den verbleibenden freien Wegen ins Einsatzgebiet gebracht werden. Gleichzeitig müssen Gefahren für die Helfer erkannt und beobachtet werden.

a) Wer nimmt daran (auch zur Beobachtung) teil, welche Beiträge haben private Firmen oder Institute hierfür erbracht, wann wurde das Projekt begonnen, wann endet es, welches Finanzvolumen hat es, und wie wird es finanziert?

Der Projektvorschlag DRIVER ist von der zuständigen Europäischen Kommission bislang nicht in eine Förderung überführt worden.

Sollte das Projekt gefördert werden, sollen Projektpartner aus Deutschland u. a. DLR (Luftgestützte Dienste zur Situationserfassung, Verkehrsinformationen, Katastrophenhilfe, Technische Leitung der Experimente und finalen Demonstration), FhG und THW (Technisches Hilfswerk) sein.

b) Aus welchem Grund interessiert sich das DLR für die Mitarbeit bei Driver?

Das DLR engagiert sich seit langem erfolgreich in der Erforschung und Verbesserung des Krisenmanagements bei Katastrophen (vgl. z. B. die Mitarbeit bei UN-SPIDER und der International Charter Space and Major Disasters). Das Know-how des DLR im Bereich des Krisenmanagements und der Nutzung von luftgestützten Diensten bei Katastrophen soll daher auch in das Projekt Driver eingebracht werden.

c) Worin besteht der Beitrag des DLR?

Das DLR möchte in Driver den Einsatz von luftgestützten Diensten zur schnellen und präzisen Lageerfassung in Katastrophengebieten, der Datenaufbereitung für die Rettungseinsatzplanung sowie der schnellen Koordinierung von Hilfseinsätzen erforschen.

d) Inwiefern will das DLR auch Ergebnisse seiner Forschungen zu Drohnen einbringen, etwa aus dem EU-Forschungsprojekt DeSIRE?

Das DLR untersucht u. a. die Integration von unbemannten Luftfahrtsystemen in den Luftraum und bringt seine bisher gewonnenen Erfahrungen auch in das Projekt Driver ein.

e) Worin besteht nach Kenntnis der Bundesregierung der Beitrag der Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V. bei Driver?

Seitens der Fraunhofer Gesellschaft wurden Anträge an die EU gestellt, um an diesem Projekt teilzunehmen. Diese sind jedoch erst in der Antragsphase und können somit nicht genauer bezeichnet werden.

f) Auf welche bereits vorliegenden Ergebnisse früherer Forschungen wird vom DLR und der Fraunhofer-Gesellschaft nach Kenntnis der Bundesregierung zurückgegriffen?

Das DLR greift auf Forschungsergebnisse zur Integration von unbemannten Luftfahrtsystemen in den Luftraum und zur Koordinierung von Hilfseinsätzen bei Katastrophen zurück. Hinsichtlich der Fraunhofer Gesellschaft liegen der Bundesregierung keine Informationen vor.

g) Wer gilt bei Driver als Koordinator, und wer sind die „Endnutzer“?

Koordinator bei Driver soll ATOS Spain werden. Zu den Endnutzern sollen ARC (Austrian Red Cross Research GmbH), MSB (Swedish Civil Contingencies Agency), THW, DRC (Danish Red Cross), BRC (British Red Cross), MDA (Magen David Adom) gehören.

h) Inwiefern ist nach Kenntnis der Bundesregierung beabsichtigt oder wird als Szenario erwogen, Driver auch bei Protesten oder zur „crowd control“ einzusetzen, wie dies nach Kenntnis der Fragestellerinnen und Fragesteller vom DLR auf der Konferenz „Angewandte Forschung für Verteidigung und Sicherheit in Deutschland“ der Deutschen Gesellschaft für Wehrtechnik e. V. in Berlin vorgetragen wurde?

Driver ist ein Projektvorschlag für den Bereich des Katastrophenschutzes zur Lageerfassung und zur Planung von Hilfseinsätzen. Ein Zusammenhang mit „Crowd-Control“ besteht nicht und wurde vom DLR auf der zitierten Konferenz auch nicht vorgetragen.

20. Wie bewertet die Bundesregierung die Notwendigkeit von Driver?

Das 7. Forschungsrahmenprogramm ist ein Programm der EU. Die Durchführung obliegt der Europäischen Kommission, die auch die fachliche Bewertung und Auswahl von Projektvorschlägen vornimmt.

21. Inwiefern ist das BKA weiterhin mit dem Institut für Sicherheit und Gesellschaft der Albert-Ludwigs-Universität Freiburg oder dem Software-Konzern IBM in Kontakt (Bundestagsdrucksache 17/13441), und zu welchen „weiteren gemeinsamen Aktivitäten“ hat die Besichtigung der „Crime Information Platform“ durch das BKA geführt?

    Welche weiteren „Informationsbesuche“ oder sonstigen „Beobachtungen“ hat das BKA bei anderen Einrichtungen zu „prediktiver Software“ vorgenommen?

Wie auf Bundestagsdrucksache 17/13441 dargestellt, wurde das BKA 2012 vom interdisziplinären Institut für Sicherheit und Gesellschaft der Universität Freiburg zu einem Informationsbesuch eingeladen. Im Rahmen des Besuches wurden auch Möglichkeiten der Zusammenarbeit unverbindlich erörtert. Unter anderem wurde von der Firma IBM die sog. Crime Information Platform vorgestellt.

Der Besuch hat bisher zu keinen weiteren gemeinsamen Aktivitäten geführt.

Das BKA hat keine „Informationsbesuche“ oder „Beobachtungen“ bei anderen Einrichtungen zu „prediktiver Software“ vorgenommen.

22. Worin bestand nach Kenntnis der Bundesregierung der Austausch Europols mit dem Department of Homeland Security zu als „Fusion Center“ bezeichneten „Terrorismusabwehrzentren“ (Bundestagsdrucksache 17/14833)?

Der Bundesregierung ist 2012 bekannt geworden, dass es einen Austausch zwischen Europol und dem Department of Homeland Security (DHS) gab, der auch die Vorstellung der Arbeit sog. fusion centers für das DHS beinhaltete. Worin dieser Austausch im Detail bestand, ist der Bundesregierung nicht bekannt.

23. Auf welche Weise sind Strafverfolgungsbehörden des Bundes mit der Prävention oder Schutzmaßnahmen von Kritischen Versorgungsdienstleistungen der Branchen Elektrizität, Gas und Mineralöl befasst, und welche Kooperationen oder Forschungsprojekte sind die Behörden hierzu mit den Betreibern Kritischer Infrastrukturen sowie deren Fach- und Branchenverbänden eingegangen?

Das BKA erstellt anlassbezogen Gefährdungslagebewertungen für einzelne Bereiche der kritischen Infrastrukturen im Hinblick auf eine Gefährdung aus dem Bereich der politisch motivierten Kriminalität. Diese werden den für Prävention/Schutzmaßnahmen zuständigen Behörden für deren Aufgabenerfüllung zugeleitet.

Das BKA ist keine Kooperationen bzw. Forschungsprojekte mit Betreibern kritischer Infrastrukturen sowie deren Fach- und Branchenverbänden eingegangen.

24. Inwiefern treffen Berichte zu, wonach die Bundeswehr mittlerweile über eine neue mobile Überwachungsplattform „Mobiles Geschütztes Fernmeldeaufklärungssystem (MoGeFA)“ der Firma Plath GmbH verfügt (www. bundeswehr-journal.de/2014/mobile-fernmeldeaufklaerung-in-krisengebieten)?

Der beabsichtigte Zweck des Systems MoGeFA ist die Erfassung elektromagnetischer Ausstrahlungen zur taktischen Einsatzunterstützung deutscher Kräfte in Krisen- und Kriegsgebieten. Vor der geplanten Serienbeschaffung eines solchen Systems wurde ein sogenanntes Demonstratorsystem in Auftrag gegeben, um

die Realisierbarkeit der beabsichtigten Nutzung nachzuweisen. Das „Demonstratorsystem“ befindet sich zurzeit in der Erprobung und wird operationell nicht genutzt. Für den Fall der erfolgreichen Erprobung des „Demonstratorsystems“ ist beabsichtigt, die Serienbeschaffung ab 2016 zu realisieren.

a) Wer hat die montierten Systeme jeweils hergestellt, und welche Kosten fielen hierfür an?

Hauptauftragnehmer für die Realisierung des „Demonstratorsystems“ ist die Firma Plath GmbH in Hamburg (Fa. Plath). Der Vertragswert zur Lieferung des „Demonstratorsystems“ umfasst 10,4 Mio Euro. Das „Demonstratorsystem“ besteht aus drei Aufklärungstrupps. Die benötigten drei Fahrzeuge vom Typ YAK wurden aus Beständen der Bundeswehr bereitgestellt.

b) Was ist mit der beworbenen Funktionalität der „Ermittlung vollständiger Funk-Lagebilder in einsatzrelevanten Frequenzbereichen“ gemeint?

Die bei der Nutzung von Funkverbindungen infrage kommenden Frequenzen sind aufgrund der physikalischen Gesetze der Wellenausbreitung und des jeweiligen Grades der Technik bekannt. Durch anhaltende Fernmeldeaufklärung in diesen Frequenzbereichen lassen sich Absichten, Strukturen und Bewegungen des Gegners erkennen und verfolgen. Diese Aufklärungsergebnisse liefern das „Funklagebild“ im Sinne der Fragestellung. Das MoGeFA ist dazu weder konzipiert noch in der Lage, den Funkverkehr von Mobiltelefonen aufzuklären.

c) Inwiefern trifft es zu, dass „in wichtigen Frequenzbereichen alle elektromagnetischen Aussendungen entdeckt und geortet werden“, und um welche handelt es sich dabei?

„Wichtige Frequenzen“ sind die zur Erstellung des in der Antwort zu Frage 24b beschriebenen Funklagebildes erkannten Funkfrequenzen.

d) Auf welche Weise wurden bei der Beschaffung des Systems Datenschutzbeauftragte des Bundes oder der Bundeswehr eingebunden, und was war das Ergebnis eines Datenschutzkonzeptes (sofern dies überhaupt erstellt wurde)?

Der Beauftragte für den Datenschutz in der Bundeswehr war bisher nicht in das Projekt eingebunden. Es ist beabsichtigt, mit dem Erreichen der Serienreife ein entsprechendes Datenschutzkonzept zu erstellen. Für die Erprobungsphase gelten die in der Bundeswehr gültigen Regelungen und Vorschriften.

e) Auf welchen bzw. wie vielen weiteren schwimmenden, fahrenden oder fliegenden Plattformen nutzt die Bundeswehr ähnliche Überwachungstechnik?

Die Bundeswehr betreibt Fernmeldeaufklärung in seegestützter Form auf drei Flottendienstbooten und mittels mehrerer Plattformen auf Landfahrzeugen, die den jeweiligen Einsatzzwecken angepasst sind.

25. Welche weiteren Angaben kann die Bundesregierung zu den Inhalten der „Working group on modern technology“ innerhalb der European Police Chiefs Taskforce mitteilen, die von Europol mit Blick auf die dritte „European Police Chiefs Convention“ eingerichtet wurde (Bundestagsdrucksache 17/14833)?

    a) Welche Instrumente zur „Früherkennung von Neuen Technologien“ wurden behandelt?

In diesem Kontext wurden keine einzelnen Instrumente, sondern vielmehr wurde die Bedeutung von „Früherkennung von Neuen Technologien“ für Strafverfolgungsbehörden behandelt.

b) Was ist damit gemeint, wenn die Bundesregierung von einer „strategisch-technologischen Früherkennung ohne Fokussierung auf bestimmte Technologien“ spricht?

Damit ist eine technologische Früherkennung gemeint, die unabhängig vom Betrachtungsgegenstand strategische Handlungsempfehlungen zum Ergebnis hat.

c) Inwiefern wurde das Ziel erfüllt, „ein gemeinsames methodisches Vorgehen im Erkennen und Bewerten von Neuen Technologien hinsichtlich einer potentiellen polizeilichen Relevanz im Allgemeinen zu beraten“?

Die Arbeitsgruppe wurde über die Beschlusslage (Dokument 9814/13 des EU-Rates: http://register.consilium.europa.eu/pdf/en/13/st09/st09814.en13.pdf) in Kenntnis gesetzt und befürwortete in den formulierten Handlungsempfehlungen die Unterstützung von ENLETS seitens der Europol-Mitgliedstaaten.

d) Welche seiner „methodischen Erfahrungen im Bereich der strategischen Früherkennung und Folgenabschätzung von Neuen Technologien“ hatte das BKA eingebracht?

Die eingebrachten methodischen Erfahrungen umfassten das Benennen des finanziellen und personellen Aufwandes, der mit einer umfassenden Früherkennung und Folgenabschätzung verbunden ist.



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333